ＩＴガバナンス協会の基調講演

【前提：パンフレットでの紹介文　】　（茶字は単なるコメントで講演対象外）

「ITGI　Japan　CIO　ITガバナンスセミナー」の趣旨

事例に学ぶIT統制への取り組み

～ＣＯＢＩＴは使えたのか、もしくは使えなかったのか～

日本の先進企業における米国ＳＯＸ法への対応、ならびに、日本におけるＩＴ統制への取り組みに学ぶことにより、特にＣＩＯの皆様にとって切っても切れない関係にあるＩＴ統制に、どうＣＯＢＩＴを使うべきなのか、再確認していただきます。


ITガバナンス協会　CIO ITガバナンスセミナー

CIOはIT統制にどう取り組んでいるか

～　したたかに、そして真剣に　～

2007年6月20日

JUAS　：(社)日本情報システム・ユーザー協会　主席研究員
東京海上日動火災保険(株)　特別任命参与
GIULIANI COMPLIANCE JAPANシニアアドバイザー
髙　橋　秀　敏

なお、本日の講義の内容は、個人の見解であって上記企業・団体の公式見解ではありません。

1

【１．初めに】

■1－1　：　挨拶

ご紹介を戴きました「（社）日本情報システム・ユーザー協会」の高橋秀敏です。

本日は、「ＣＩＯはＩＴ統制にどう取り組んでいるか」というテーマについて、50分の時間を戴いてお話しさせて戴きます。

まず、講演の目次をご紹介します。

(1)簡単に、自己紹介をします。
(2)次に、本日の演題のキーワードであります「ＣＩＯ」について、
ＣＩＯとは何か、その機能は？　そして、ＣＩＯとして何が必要か？
についてお話しさせて戴きます。
　また、例年、経済産業省からの委託を受けてＪＵＡＳで実施しています　「企業ＩＴ動向調査」から見えてきたものということで、アンケートの結果およびインタビューの中から、テーマに関係しているポイントをご紹介します。
(3)最後に、皆さんの「気づきのヒント」になる取り組み事例をご紹介することにいたします。

■1－2 ： この講演を聞くと何が分かるようになるのか

私の後に、各企業で推進役として活躍をされている方達の具体的な実務の話が続くので、この基調講演では、全体を概観することに力点を置きたいと思っています。
この 50 分の講演を聞くことで、何が分かるか、と云うよりも何を理解していただきたいかを挙げたのが、以下の５点です。

◎ＣＩＯとは何か
◎全社的な取り組み課題が続々と現れるが、どう整理したら良いのか。
◎また、課題への取り組みを現場にも分かりやすく浸透させていく工夫は何か。
◎そして、日本の企業のＩＴ統制への取り組みの現状をアンケートから理解していただく。
◎更に、数値だけでは見えてこない本音を、ＣＩＯやＩＴ部門長へのインタビューから理解していただく。

とは言いましても、この課題に対する回答は一つではなく、業種、業態、企業規模、そして、特に企業文化によって異なります。
従いまして、この講演では、今後のアクションプランのための「気づきの眼（芽）」を提供するのに留まります。

【２．自己紹介】

私の自己紹介は、既にセミナーの案内にも載せましたし、お手元のパワーポイントの資料をお読みいただければおわかりだと思いますので、省略します。

（省略した内容　：　茶字は単なるコメントで講演対象外）

- 2000 年以降は、情報システム部門の専門職として、システムリスク管理、品質管理に従事する。その後、活動の範囲を広げ、ＩＴ企画部の専門次長以外に、ホールディングカンパニーの文書管理部、東京海上日動火災保険（株）の経営企画部、文書法務部、リスク管理部の各部署を兼務する。
- 2006 年 6 月末で早期退職したが、2007 年 1 月からは、同社の「特別任命参与」として、社長の経団連活動などの支援に従事。
- （社団法人）日本情報システム・ユーザー協会（JUAS）の主席研究員
  企業情報マネジメント研究会の部会長、調査部会の委員
  JIPDEC の ITSMS（IT サービスマネジメントシステム）技術専門部会の委員
- 著書：「システムリスクに挑む」（共著：社団法人金融財政事情研究会発行）
  システムリファレンスマニュアル（SRM）第 2 巻」（第 5 章）「リスク管理内部統制」

ただ、本日のテーマでありますリスク管理・内部統制との私の今までの関わりについては、この場でお話ししておいた方が良いと思います。

そのためには、ＣＯＳＯのフレームワークから始める必要がありますが、皆さん、ご存じのとおり、1992 年に米国で策定されて、グローバルスタンダードになっていった訳ですが、ニューヨークで起きた大和銀行事件のように米国内の海外の金融機関の不祥事件を契機に、世界的な対策が必要という認識に立って、バーゼル委員会が 1998 年にＣＯＳＯをベースとした管理体制強化のフレームワークを作り、各国の金融監督官庁が取り入れるようになりました。

日本では、1999 年に当時の金融監督庁が、「リスク管理態勢の構築」を目的とした検査用のチェックリストを作成しました。

このときは、ＣＯＳＯの Internal Control をリスク管理態勢の構築と呼んだ訳です。

このチェックリストに沿って、各金融機関は毎年自主点検をして改善をすることが義務付けられ、数年に一度、金融庁の検査を受けることになった訳です。

そういう意味では、金融機関ではＰＤＣＡが既に６回は回っていることになるわけですが、残念ながら、まだまだ様々な問題を抱えているのが現状です。

損害保険会社は、リスク管理が本業ということで、当時、チェックリスト適用の第一号になりまして、それ以来私はシステムリスク管理を中心に担当してきました。

また、持ち株会社が米国企業改革法の適用対象であったこともあって、対策立ち上げにも関わりました。

その時の一番の悩みは、金融庁のチェックリストと米国企業改革法のリスク分析のリストを２重に作ることをいかに避けるかということでした。

これは、リスク管理担当の作る手間と言うことよりも、現場へのヒアリングや資料提出などで重複がないようにしたいということがメインでした。

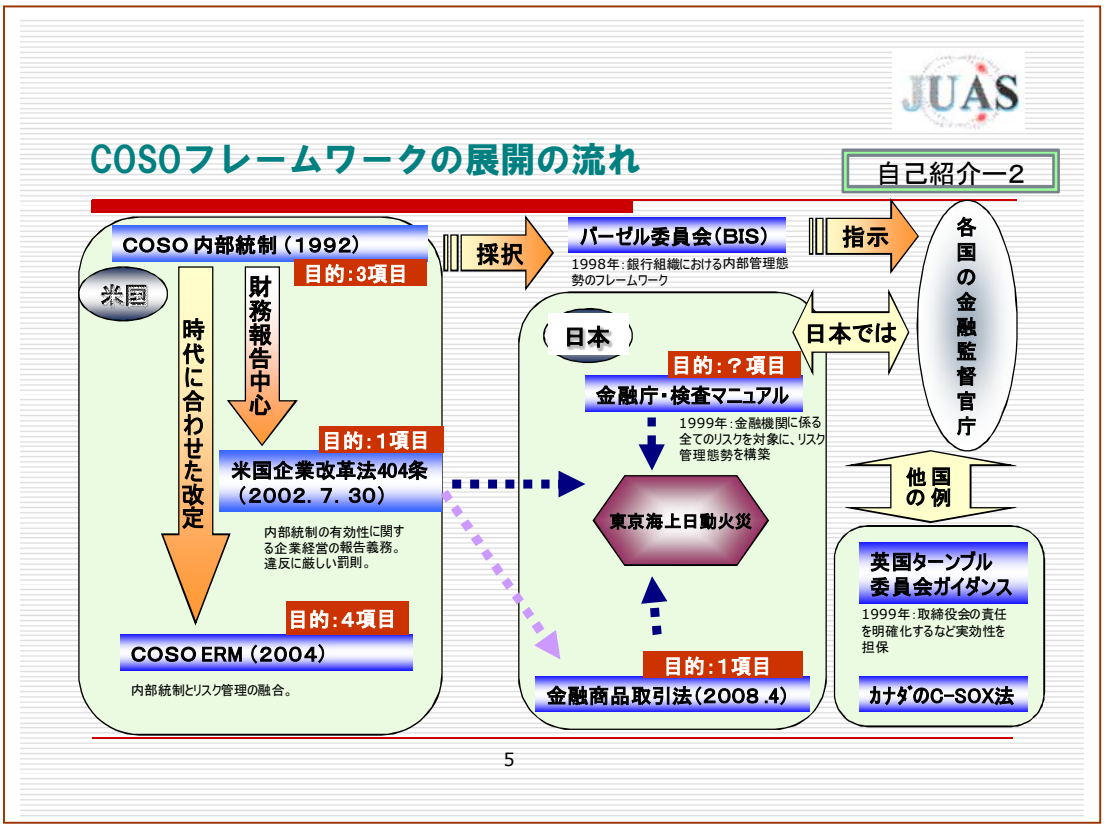
そのために、両者のチェック項目を網羅した自社版の「統合型チェックリスト」を編集しました。そして、両者のチェックリスト項目とのマッピング（紐付け）要領を明確にしたリファレンスシートも作成しました。

このときに、ＩＴ統制にＣＯＢＩＴを採用するかと言うことも検討しましたが、当時の状況では、時期尚早と判断しました。

その後、個人情報保護法の技術的安全管理措置への対応や、ＩＳＭＳ等に基づく情報セキュリティの強化など、段階的にリスク管理態勢を充実させていった訳です。

現在は、東京海上日動火災のこうした業務には全く関わっていませんが、ＪＵＡＳの主席研究員として、また、企業情報マネジメント研究会という部会の共同部会長として、リスク管理・内部統制をテーマにした活動をしています。

この部会では、３年前からリスク管理・内部統制を検討のテーマにしていまして、基礎的な学習、課題の整理を経て、2007 年度は実務で発生する問題を皆でディスカッションしながら解決していくことを主眼に活動を進めています。



【３．ＣＩＯの機能とは何か、何が必要か】

私はＣＩＯではありませんので、経験に基づくＣＩＯ論はお話しできませんが、今まで接してきたＣＩＯとディスカッションして共有してきたＣＩＯ論をお話しします。

2005 年に、経済産業省の主催で、「ＣＩＯの機能と実践に関するベストプラクティス懇談会」という会が開催されました。

各企業の考え方を聞きたいということで、東京海上日動火災からも、ＩＴ企画部の担当役員であった常務の隅（当時）が、会社の考えを説明いたしました。

本日は、その時に説明した中から、２つの話題を私なりにアレンジしてお話しします。

一つ目の話題は、ＣＩＯの機能についてですが、これを一言でいえば、「他のラインや経営層との連携と調整」ということです。

具体的なポイントは、以下の３点です。

(1)システムがブラックボックスという言い方がなされますが、ブラックボックスなのはシステムではなく、縦割りの商品や社内規定がブラックボックスを生んでいるというのが真相であると思います。

従って、全取締役が、担当分野の透明性を上げていくことが大切で、そのことが充分に果たされるならば、それを支えるシステムの透明性も高まり、最終的に、コンセプトの明確なシステムに結実していくと言えます。

(2)次に、システム開発の規模が膨らんでいくのは何処に原因があるのかということですが、依頼する部門（アプリケーションオーナー）の精緻主義・完璧主義によって、システム化の要件が肥大化することが真因だと思っています。ＣＩＯのミッションは、過剰な開発を抑止するために、精神論だけでなく、仕組みを設けることであると思います。（例として、プロジェクト策定時の第三者による審査・評価のスキーム導入、予算のしばり　など）

(3)ＣＩＯのミッションを考える上で、一番重要なこと。それは、ＩＴのことはＩＴ担当役員に任せるということでは、実効ある経営戦略の策定が出来ない時代に入っていることです。このことは、昨今会社法に説かれている条文を見ても皆さん十分お分かりの通りだと思いますが、まだまだ、システムのことはわからない、ＣＩＯに任せているという本音を耳にします。言い逃れの材料としてのＣＩＯならば、不要と言った方が正しいと思っています。

今、経営に求められているのは、縦割り組織から出てくる様々な判断に、横串を入れた経営判断をすることですから、取締役全員がＣＩＯという認識が大切だと思います。その上で、本物のＣＩＯが生まれて力を発揮していく風土が、日本にも定着していってほしいと思います。

次に、「ＣＩＯ的立場として必要なもの」として、以下の３点を挙げました。

⑴ＩＴ＝経営 ということがよく言われますが、掛け声だけのケースが大半です。これでは、横串の入った経営体制を作るのは至難の技で、ＣＩＯの最大の使命は、如何に、このコンセプトを、全経営陣の**「肚に落とし、実行する」**ということに尽きます。
⑵そのために、ＣＩＯとしては、ＩＴ技術よりも、経営の課題に対する幅広く深い見識を持つことが前提になります。そして、その上に、経営とＩＴを結びつける洞察力と理解力が重要です。
逆に、有能な技術者からのヒントを生かせるセンスがあれば、ＩＴ技術の専門的知識をＣＩＯが自ら持つ必要はないということでもあります。
⑶更に、絡み合った分かりにくい問題を、自分の言葉で分かり易く納得させる能力が大切で、現状をビジュアルに説明することで初めて「肚に落とす」ことが可能となります。

机上のＣＩＯ論は意味がないのでストレートな表現を使いましたが、その意図するところをご理解いただけたものと思います。

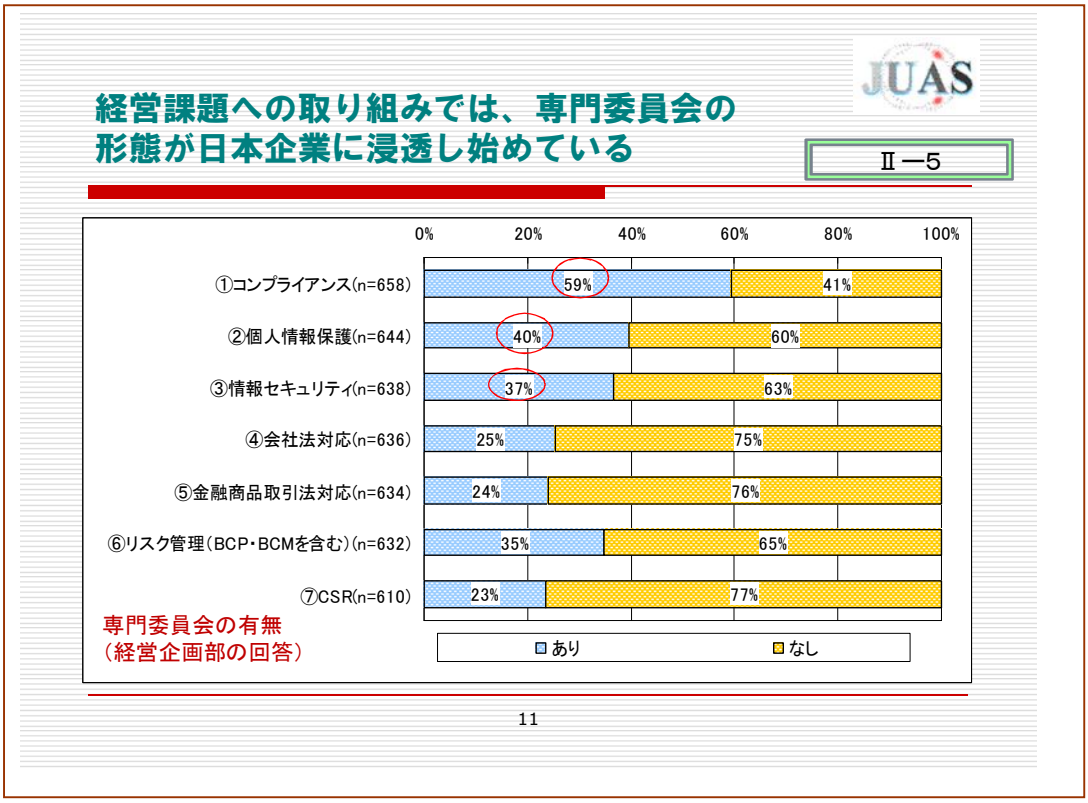
次に、「企業ＩＴ動向調査」の話題に移ります。

【４．ＪＵＡＳの企業ＩＴ動向調査結果から見えてきたもの】

ＪＵＡＳの企業ＩＴ動向調査の概要については、お手元のパワーポイントに解説していますので、後ほどお読みください。
ポイントは、３点ございます。
⑴アンケートの対象企業が４千社近くあり、有効回答も８００社あって、母集団としては信頼のおける数が集まっていることです。
⑵次に、ＩＴの動向調査ではありますが、ＩＴ部門だけでなく、依頼部門である経営企画部門にも回答を求めて同じく８００社からの回答を得ていることです。
⑶そしてアンケート結果の数字からは見えてこない現状を、インタビューで集めていることです。先進的な取り組みをなさっているユーザー企業のＣＩＯ、ＩＴ部門長、そして、内部統制の担当部門の方を対象に計５０社の生の声が集まっています。
調査レポートは、数センチの厚みがありますので、詳細はお読みいただくとして、まずは、本日のテーマに直接関係ある結果をピックアップして、お話します。

■4－1 ： 経営課題への取り組み状況

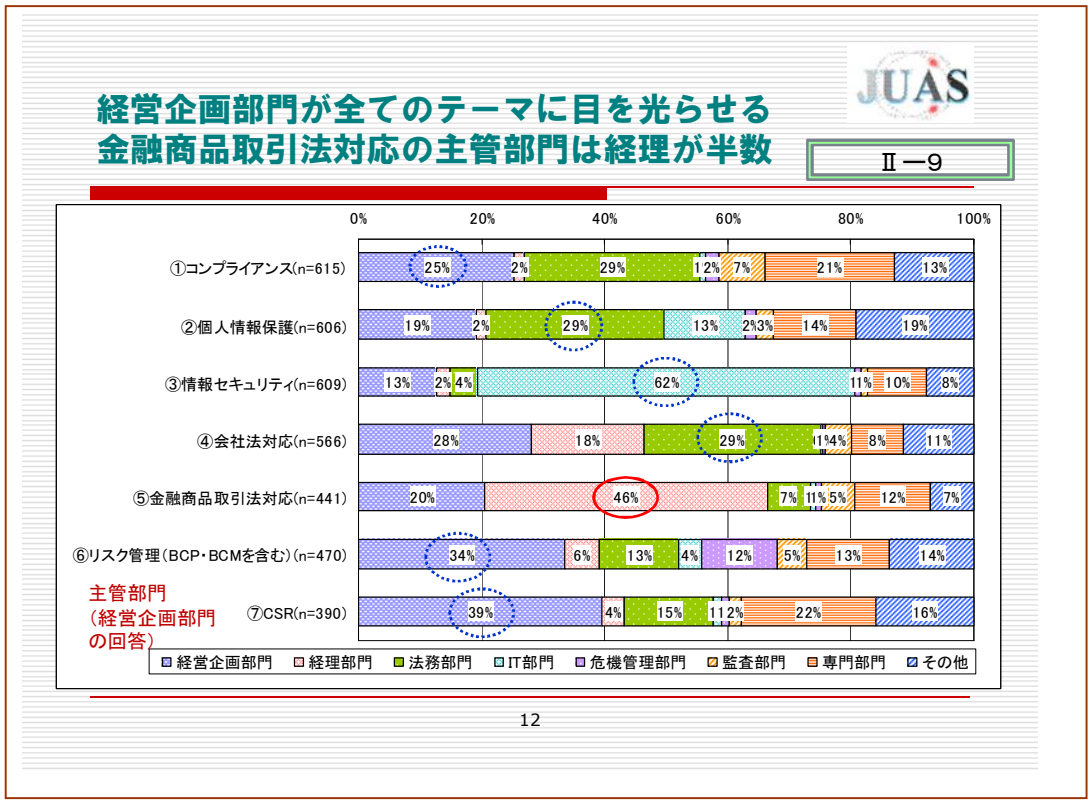
(1) 一つ目は、経営課題への取り組みに関して、「専門委員会の形態が日本企業に浸透し始めている」ということです。
経営課題と言っていますのは、このパワーポイントに掲げた７つであります。
「①コンプライアンス」、「②個人情報保護法」、「③情報セキュリティ」、「④会社法対応」、「⑤金融商品取引法対応」、「⑥リスク管理（ＢＣＰ(Business Continuity Plan)およびＢＣＭを含む）」、「⑦ＣＳＲ（Cooperate Social Responsibility）」です。



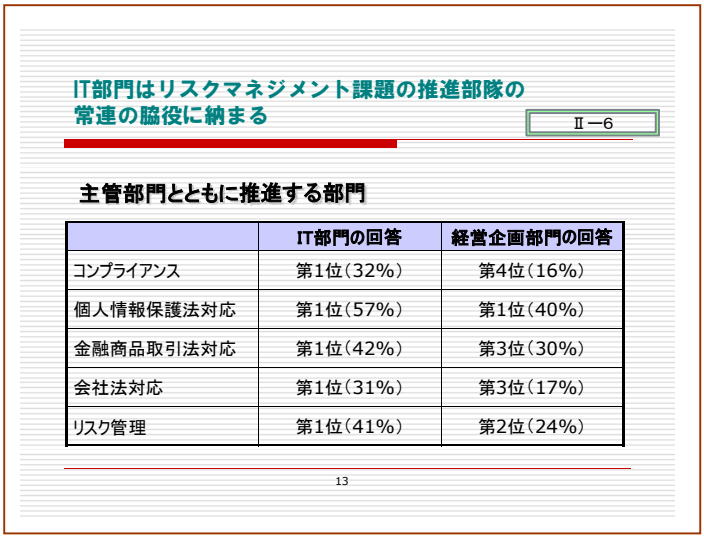
結果は、「コンプライアンス」が一番浸透していて６割あります。それ以外の課題については、大きく２つに分かれまして、「個人情報保護法」「情報セキュリティ」「リスク管理」が４割程度、新しい３つの課題は25%程度といったところです。

以上が、専門委員会についてですが、それでは具体的に、どのような部門がそれぞれの課題の主管部門になっているかという点について、お話します。

(2)主管部門については、経営企画部門が全てのテーマに目を光らせています。第一位ではなくても、必ず上位に位置しています。これは当然かもしれません。
因みに、金融商品取引法対応の主管部門は、経理部門が46%と約半数を占めています。



(2)今回のアンケートの中で、私が一番知りたかったのは何かと言いますと、ＩＴ部門が経営に貢献しているとよく言われていますが、本当に社内でそのように認識されているか、本音の評価がどの程度なのかということであります。
情報セキュリティのように、
技術面の課題として、ＩＴ部門が主管部門になっている課題を除くと、このパワーポイントのような結論になりました。
ＩＴ部門が、自らを、協力部門の常にトップとして挙げているのは、意気込みと自負とも受け取れますが、一方、経営企画部門からは、必ずしもそこまでの評価は与えられていません。
ただ、一位ではないものの、



それなりに脇役として評価はされているということだと思います。
今後、この結果が、定点観測していく中でどのように変化していくかを楽しみにしたいと思っています。

(3) 日本版ＳＯＸ法のアンケート結果では、推進にあたっての悩み（上位 3 位までを選択）という質問項目で、ダントツの一位は「どこまで対応すればよいか分からない」という回答でした。各企業の進行状況にバラツキはあっても、最終的にはこの根源の悩みに辿りついているようです。
昨年の１１月末時点では、「文書化およびメンテナンスの作業量が膨大、どこまで費用をかければよいのか、具体的作業に落とす指針がない、ＩＴ対応の要件が不明確」などの具体的な項目が挙がっていました。
こういう案件は、まずはやってみましょう、パイロット的に進めてみて、その経験を基に対象を広げていけば、段々見えてくるという読みで進めることが多いのですが、本件、必ずしもそのような事態にはなっていません。
最近、米国企業改革法対応を終えた会社さんにもお話を聞く機会があったのですが、「対応を終えた後の一番の悩みは何ですか」という質問に対して、「どこまでやればよいのかわからない」という回答が返ってくるケースが幾つかありました。
自社なりに考え方を整理して進めてみたものの、監査法人からの予想外の指摘対応に振り回されたり、最終局面で監査法人の方針がころころ変わったりして緊急対応が発生したことがあったとのことで、振り返るとともに、今後のアクションプランを立案するに当たっても、どう練っていくのか、拠って立つところがわからなくなっているようです。
このテーマ、まだまだ霧の中を走り続けることになりそうです。

■4－1 ： CIOの動向調査結果

次に、ＣＩＯの動向調査の結果、これは昨年の調査ですが、参考になりそうな点を３つお話します。

(1) ＣＩＯがどの程度設けられているかを、企業規模別に見てみました。
結果は、ＣＩＯを設けている企業は、全体の８％に留まっています。逆に、ＣＩＯがいない、あるいはＣＩＯに対する認識が無いという回答をしている企業が、47%、約半数います。
ただ、この値は、企業規模によって大きく変わります。従業員１万人以上の企業規模では 27%の企業でＣＩＯを設けていますし、ＣＩＯはいないという回答も７％と非常に少なくなっています。

⑵次に、ＣＩＯが不安に感じている点ですが、一番の悩みは、「ＩＴ人材の育成と管理」であります。そして、「内部統制」、「業務改革」「ＢＣＰへの対応」が続きます。

⑶ＣＩＯとしての責任を果たす上で悩んでいる点は、ダントツで７割の方が「ＩＴ投資の適正規模が不明、可視化が難しい」という点を挙げていらっしゃいます。

以上が、日本のＣＩＯの平均的な像であります。

■4－4 ： CIO／部門長へのインタビュー

本年２月前後に実施したＣＩＯ/部門長へのインタビュー（約５０社）を実施してみての率直な印象は、**「したたかに　そして真剣に」**取り組んでいるということでした。

対象企業は、それぞれに特徴を持っていらっしゃる先進企業ですから、平均像とは異なりますので、こうした事例もあるということでお聞きください。

アンケートからは見えてこない微妙な本音ですので、脚色をせずに、生の形で幾つかご紹介します。

ところで、この「したたか」というのは皆さんどう受け止められたでしょうか。

良いニュアンスの言葉ではないのに何故？という質問を受けましたが、この言葉、奈良時代に、「気丈な人」「確か（しっかりしている）」という意味で使われ始めた褒め言葉でしたが、明治時代に意味が変化して、「一筋縄ではいかない」というマイナス・イメージが付け加わったそうです。

本講演では、「一筋縄ではいかない」という意味も褒め言葉と思って使っています。

まずは、ＩＴ部門の果たす役割と人材についてです。

⑴先程のアンケートで、ＩＴ部門が社内において脇役として存在感を発揮しているという話をしましたが、或る部門長からは「主管部と共に推進する部隊として大きく位置づけられるのは良いが、職責を果たすべく、経営的な観点からリーダーシップをとれる人がＩＴ部門には非常に少ない。共に推進するというよりも、主管部から言われたことを忠実に実行する優秀な部隊というのが、まだまだ実状である。」という厳しい発言がありました。このことも含めて、ＣＩＯの一番の悩みが、「ＩＴ人材の育成」として挙がってきているのだと思います。

⑵別の部門長からも、「内部統制・リスク管理に従事してきた人は、地味な人が多く、かつ団塊の世代の退職などもあって、体制から外れていっている。そういう人材が圧

倒的に少なくなっている現状に反比例して、経営からのニーズが急速に高まってミスマッチが発生している。」という意見も挙がっています。求められているのは、ＩＴ部門の従来の業務とは異質で、ＳＥ的なことよりも、経営の観点、法律面の素養などです。監査法人の人材育成が喫緊の課題として挙げられますが、その対応窓口となり社内の推進の核となるキーパーソンがおらず、また育成の計画自体も殆ど白紙の状態ですぐには今後の見通しが立っていないという実態は、より深刻だと思います。

(3) こうした課題解決を通して、ＩＴ部門の存在感を高めることに成功して、自信を深めたＣＩＯの例もお話しします。

「ＩＴ部門が全般統制について責任を持ち、ビジネスプロセスについては、プロセスオーナーが責任を持つという分担にしている。しかし、ビジネスプロセスが全部分かっているプロセスオーナーはいないし、システムとの絡みは更に分からないので、ＩＴ部門が全面的にサポートしなければいけない局面の割合が極端に多い。こうした背景から、先行実施したパイロット業務を通して、ＩＴ部門がプロセスの不備などを指摘できるようになってきた。更に、ＣＯＢＩＴやＩＴＩＬ等のワールドワイドのフレームワークをＩＴ部門は持っており、どのあたりに過不足があるのか、自社のプロセスはかくあるべきという観点から、海外拠点も含めて内部統制を随分と見直した。今や、ＩＴ部門は、主役に代われる実力を備えてきたと考えている。」

次に、日本版ＳＯＸ法対応における悩みについての発言を２つそのまま挙げます。

(1) 日本版ＳＯＸ法がスタートする局面では、経営としても重要性に鑑み、初期の投資を認めてくれるが、この課題は積み残しを抱えながら、それ以降毎年改善を図って充実していかなければならないと考えている。却って、初期費用に多額のものを積むよりも、ＩＴ部門への総額の投資を数年間で山崩し出来るように経営の承認を得ておくことが、経営からのリクエストに真に応えられるものと考えている。過熱した風潮に踊らず、控え目にしていく。そのために、初年度の今年は、ＩＴ部門が自力で出来るものは自ら実施する姿勢を示していくことにしている。

(2) 主管部は経理部なので、経理部と監査法人との打ち合わせ結果を踏まえた指示が出されれば、ＩＴ部門としてその対応をすると思えば、敢えて悩む必要は無いと考えている。その分、限られたソースをより効果的に投下するためには、ＩＴ部門が責任部門となる他の経営課題（例えば情報セキュリティなど）にもっと検討のロードを注力したい。

最後に、全体を見ての回答と私のコメントです。

(1) 日本版ＳＯＸ法対応に熱心に取り組んでいらっしゃる企業でありながら、要する費用が少ない、中にはゼロというアンケート回答があったので、その間の事情をお聞きしました。グローバルな企業では、欧米の対応と歩調を合わせて進めるために、数年

前からＩＴの大改造を始めていらっしゃるケースが多くあります。丁度一段落したところで、今年のＩＴ投資も内部統制に投じるものの、「今までの流れでずっと階段を上がってきたところの最終段階を、少し前倒しで実施できるようになったということ」だそうで、「何も日本版ＳＯＸ法のためにすることではない」という認識に立っていらっしゃいます。

グローバルになればなるほど、一つの国の事情で個別に対応することは認められにくく、世界の動向を見ながら一歩先んじた手を打つことが求められてきていると言えます。

なお、先ほどアンケート結果の数字の信頼性について触れましたが、こうした経営課題のような微妙なテーマは、実態と名目（本音と建前）で乖離することがあるので、気をつける必要があるということを学びました。

(2)多くの企業の回答には、予想していた「錦の御旗」というキーワードがやはり出てきました。ただ、積極的に使おうとしているのかというと、「元々、やらなければならない課題があったが、日本版ＳＯＸ法が見直しのきっかけとなり、必要があれば錦の御旗として使えることがメリットである。」という回答が大半でした。

どのように使うかは、各社各様ですが、例えば、「開発・運用の標準化」「ドキュメント整備」「セキュリティ、ログ監視、データ保存」、「ＥＡの導入」「ＣＯＢＩＴの導入」「ＩＴＩＬの導入」など、それぞれ実施したい対応策と絡んだ回答が挙がってきます。

(3)内部統制の取り組みはネガティブに受け取られることが多いので、ＩＴ部門から見たプラスの面もお聞きしましたが、たとえば以下のような回答がありました。

・業務とシステムの意味づけが明確になった。
・改善案の創出の情報源になった
・基幹業務再構築時の、改善のネタにつながる項目が出てきた。

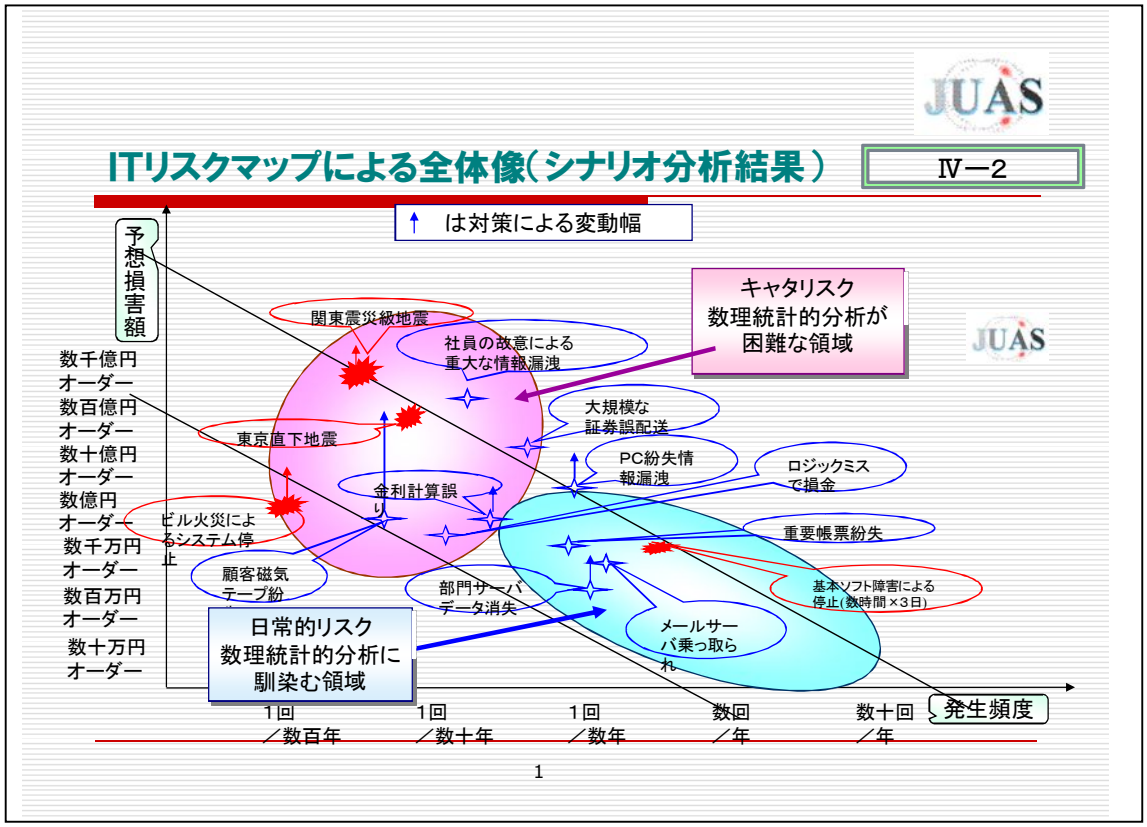
【５．私からのメッセージ】

ＣＩＯ論とか経営課題の取り組み状況と言った解説は、この程度にしましょう。
自己紹介でお話したとおり、この数年間リスク管理担当として取り組んできましたが、その中から、皆さんの気づきのヒントになりそうな話題をいくつかご紹介します。

■5－1 ： 日頃からリスクを認識・分析・評価する訓練をする。

私からのメッセージの１番目は、リスクに対する感性を日頃から磨くことの大切さについてです。

(1) リスク管理は難しい話ではありません。
必要なのは、「リスク認識の感性を磨くこと」、「リスクシナリオの作り方を学ぶこと」、「素因数分解の思考パターンを身につけること」、「１枚の絵でリスクの全体像を描いてみること」などの訓練で、各々数時間も話せば基本は身につくことです。
本日は、時間の関係で、その中の一例として、「企業のシステムリスクの全体像を描いてディスカッションすると、企業としての共通の認識が生まれる」という例を話します。



これは、リスクマップです。皆さん本などでよくご覧になっていらっしゃると思いますが、単に担当者の分析ツールとしての役割で終わっていないでしょうか。

この図を、経営者に理解してもらう、先ほどの言葉でいえば、全経営陣の**「肚に落とし、実行する」**ということに活用できないかということです。

リスク分析結果の全体像は、図のように縦軸を予想損害額、横軸を発生可能性として整理してみますと、幾つかの事象をプロットしてみますと、「巨大リスク」と「日常的なリスク」との２つに大別されます。

「巨大リスク」とは、発生頻度は高くはないが、発生すると予想損害額が大きい事象です。従って、ベースとなる統計数字が乏しいので、シナリオ分析の手法を用います。

一方、「日常的なリスク」については、トラブル記録からリスク要因や頻度分布に関する分析が可能であり、その分析を経て有効なリスク対策を洗い出していくことができます。

ポイントは何かというと、一つの事象にも前提があり、その前提次第では、損害額が増えたり、また対策を講じておけば抑えることができるということなのです。

例えば、ビル火災でも、名古屋支店なのか、新潟支店なのかによって差が出てきますし、安全対策のレベルでも異なってきます。その変動幅を合わせて明示しておくことです。そして、ベストシナリオに移行させるためにはどうしたら良いか、いくら投資が必要なのか、ワーストシナリオはどうすれば回避できるのか、いくらかければ何処まで改善されるのかということも、この図に矢印で書き込むことによって、全体最適の観点からアクションプランをどう取るのが望ましいのかなどの論議も一枚の図でできるようにしておくことです。

こうして作成した図を、経営陣に提示して、ディスカッションしてもらうと、皆さん、それぞれ頭に描いている発生頻度・損害額とも異なりますが、それぞれの見解を述べていくうちに、意見がまとまっていきます。

正解は元々ありません。見解の相違をディスカッションすることで、経営陣が一つのリスクの認識を共有することができれば良いのです。経営にとって会社全体の抱えるリスクの全体像を見ながら、リスク認識・分析のコミュニケーション・ツールとして用いることが、とても重要だと思っています。

こうして、この図表で、経営として容認できない事象のリスク対策の優先度を、ディスカッションのアウトプットとして受け取ることができます。

オーソライズされた対策は、リスク管理のアクションプランの計画に盛り込んで、推進していくことができます。

こういう図を一度作っておくと、何度も作成する必要はありません。

個別に、例えば、情報セキュリティ対策を立案するときに、同じように１枚のリスクマップに描いて、グループ毎にカテゴライズし、リスク認識とアクションプランを決めていくようにすればよいのです。

⑵ 同じように全体像を描きながら、プロジェクトを進める大切さという観点から、もう一度ＣＯＳＯのフレームワークに戻って、「Ｔ字型・Ｉ字型」のお話もしておきます。

ＣＯＳＯには、３つの目的があったということは皆さんよくご存じのことでしょう。「業務の有効性・効率性」、「財務報告の信頼性」、そして「コンプライアンス」ですが、2002 年 7 月 30 日の米国企業改革法は、「財務報告の信頼性」という一つの目的を深く掘り下げていくことになったわけです。そういう意味では、ＣＯＳＯが浸透していって企業活動に必要な目的をカバーした上に、一つを掘り下げる縦横の「Ｔ字型」の解決が、米国および日本の一部の企業では行われているということです。これが、目指す姿ではないでしょうか。ＣＯＳＯのフレームワークに慣れる間もなく「財務報告の信頼性」という一つの柱に絞っていきなり掘り下げることになる多くの日本企業は、「Ｉ字型」の解決にならざるをえません。

そのことの弊害は、全体の経営課題の中での位置づけが分からず、「どこまでやればよいかわからない」という悩みにつながります。

因みに、ＣＯＳＯのＥＲＭでは、更に戦略を目的の一つに加えて、横に幅を広げようとしています。

この「Ｔ字型・Ｉ字型」のお話は、２年ほど前からＪＵＡＳの研究会でも話をしているのですが、時間が限られてきた現時点でも、是非、長期的な課題であるだけに、広く見ることを忘れないで戴きたいと思います。

⑵次に、お話ししたいのは、経営には、日頃から、リスクに関する情報を提供して、身近に感じてもらうことが大切であるということです。

日々新聞報道される事件などは、検討の宝の山だと思いますし、私自身、活用して効果を挙げた実例もあります。

本日は、一寸目先を変えて、ジュリアーニ氏の取り組み事例を取り上げます。

ジュリアーニ氏というと、ニューヨークの元市長で、犯罪を激減させたり、最近では共和党の大統領候補として名前が挙がったりしますが、彼を有名にしたのは、9.11 のあの事件です。

彼が陣頭指揮を取っている映像は皆さんの印象に残っているでしょうが、私もあの映像を見たときに、エネルギッシュな方であると同時に、流石政治家らしくパフォーマンスの上手な方という印象を受けました。

しかし、昨年暮れに彼が来日して講演した内容を聞いて、認識を改めました。

彼は、市長の時代に様々な事件などを俎上に載せて、全スタッフで対策のシミュレーションを重ねていたのだそうです。サリン事件も、ニューヨークの地下鉄で起きた場合にどう対応するかを検討したそうです。

あの 9.11 事件は未曾有の惨事でしたから、そのレベルまでのシミュレーションはしていなかったと語っています。しかし、シミュレーションを重ねたお陰で、会議のメンバーが、この惨事にどのような行動をするかは彼には読めていたそうです。あの人ならば、きっとこうしている、また別のあの人ならきっとあそこに駆けつけているということが手に取るように一瞬にして読めたので、対策本部に招集をかける必要はなく、彼自身も最前線に駆けつけて、自分のなすべきことに専念できたそうです。

これはなかなかすごいことだと思いました。リスクは発現してからでは遅いです。日頃から、様々な事例を基にシミュレーションして事前に対策を講じ、そして実際に起きたら迅速に対応する、このことが今本当に大切になっています。

■5－2 ：「身の丈に合った」内部統制で「全体最適」を目指す。

私からのメッセージの２番目は、「身の丈に合った仕組み」についてです。

これは、組織の話でありますが、昔のように、人事、総務、経理といった部門が、それぞれの分掌業務を、特段の分野調整も無く遂行できた時代は過ぎ去っています。

経営課題全般に当たって、委員会を設置するのか、プロジェクトチームを編成するのか、オールラウンドな経営企画部門が主管部となって推進するのか、いろいろな形態が考えられるわけです。今一番変化の激しいこうした経営課題への取り組みの推進の実態を知りたくて、アンケートの中に質問項目を入れてみました。

(1)結果は、各企業によって千差万別でした。ただ、企業毎にポリシーは明確で、話を聞いてみると納得する部分が多く、レポートのタイトルは、「経営課題への取り組み姿勢は企業風土を映す鏡」としました。

先ほど「「専門委員会の形態が日本企業に浸透し始めている」と言いましたが、これが果たして良い傾向なのかということについて、少しコメントします。

これだけの数の委員会が乱立して十分に機能しているのかということが、素朴な疑問でした。

実態は、やはり、各委員会で相互に依存しているケースがかなりありました。或る委員会は別の委員会の下部組織になって階層構造があったり、その事務局のメンバーは大半共通であったりして同じような資料に基づいて論議がなされていたりということになっています。その結果として、 対策の重複感や度重なる変更、および現場への複数の指示による混乱を懸念しています。

これでは、本来の業務改革のスピードが実現できなくなるのではないかと思います。

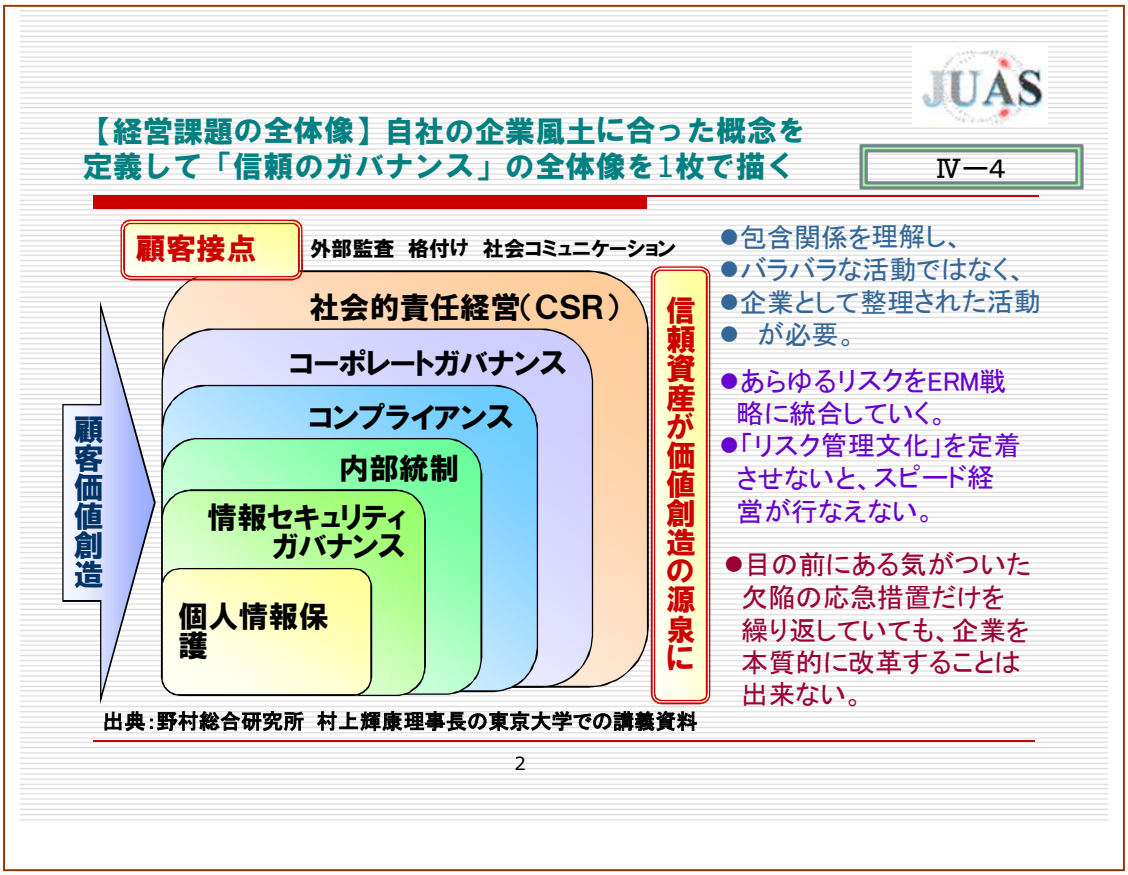
(2)解決のためにお勧めするのが、「自社の企業風土に合った概念の定義をして全体像を１枚で描く」ことです。

これだけ隣接する概念が何本も競い合っている時代ですから、ラフでよいのですが、各社で一度全体像を整理してみることが有効になります。
と言うのも、社内各部署で異なった概念を頭に描いて混乱が生じないように、各社なりに使用する言葉を明確にして、全社員に分かりやすく説明できるようにしておく必要があるからです。
気をつけなければならないのは、各社各様だからと言って、自由に定義できるかというと、時代の流れが大きく変わっていく度に見直しが求められることです。
例えば、情報セキュリティ（情報の機密性・完全性・可用性）の定義ですが、内閣府情報セキュリティセンターが、様々な活動を精力的に進めていますが、そこでの定義は、当初のサイバー攻撃からスタートして、今では、災害、非意図的要因、「ＩＴの機能不全が引き起こすサービスの停止や機能の低下等」（ＩＴ障害）といった範囲まで対象を広げてきています。どんどん定義が変わっていくので、社内の定義でも配慮が必要になっていきます。
こうした諸概念を、全体像を１枚で描くときの事例として紹介するのが、野村総研の村上理事長が東京大学で昨年講演されたときに用いた「信頼性のガバナンス」の図です。（次ページ）
図が示しているのは、情報セキュリティ　→　内部統制　→　ＩＴガバナンス　→　ＣＳＲの順番で範囲が広がっていくことでして、厳密には、プロセス、マネジメント、ガバナンスは次元の違う概念なので比較しようがないということも言えますが、カバレッジの大きさということで理解していただきたいと思います。重要なことは、入れ子構造になっていることです。
各言葉の定義の違いを論じても意味がなく、包含関係が逆転しても良いのですが、要は、複雑な相関を止めて単純な包含関係が成り立つように、言い換えれば、境界線が明確で範囲が重ならないようなイメージにまずは簡単にまとめておくことが、全体像を説明するのに良いということなのです。
そうすることで、各課題と直結する企業内での推進組織や対策が重複せず、組織間のインターフェイスで取られる時間の無駄を廃除し、一貫した判断を可能にするにはどうしたらよいかと言う課題のヒントになります。社内の体制を思い浮かべながら、シンプルに表現することにトライしてみてほしいのです。

私がこの図を用いて知りたかったのは、金融機関しかイメージが湧かないので、業態が異なるとどのように違ってくるかということです。
リスク管理・内部統制で、金融機関は特殊で参考にならないと言われるのですが、果して何が異なるのか、お互いに益する部分はないのかという疑問を持ち続けてきました。
最初は、メーカー系の方達とは意見が合いませんが、１～２時間もディスカッションしていくと、段々と、業種によらない部分、各社固有の部分などが見えてきますし、文

殊の智恵で、自社の経営環境や風土に合った各企業なりのラフなイメージが湧いてきます。

一つの業界に閉じずに、様々な異業種の方達と接してみると、自分の立ち位置が見えてきて、更に全体像が明確になっていくように思います。



(3)　「身の丈に合った」内部統制で「全体最適」を目指す　ということに関して、次にお話したいのは、自主点検についてであります。

先程、金融機関は自主点検がベースになっているというお話をしました。

今から振り返っても、自主的に改善していく仕組みが無いと取り組みが長続きしませんし、ＩＴ分野の技術的な問題は外からは分かりにくい部分が多くありますし、現場の担当は気が付いていることが多いのでその知見を大切にするということ、更に、ベテランによるチェックもまだ暫くは有効に活用できる状況にあると思います。

その上で、内部監査部や外部の監査人からのアドバイス・指摘を受けながら、充実させていくことが本来の姿ですし、レベルの高い管理態勢を構築することができると思います。

こういう話をしますと、意義は理解できたが、具体的にどのような手順で実施すれば良いのかという質問がでてきます。
問題解決の「打ち出の小槌」のように受けとめられるようで、特殊な手続きやチェックシートがあるだろうから、そのノウハウを教えてほしいというものです。
この具体的な自主点検の要領については、システム・リファレンス・マニュアル（ＳＲＭ）に記述しましたので、参照してください。
一言で言えば、「直面する課題に即して考える」こと、「外部監査の指摘を受けてのレベルアップ」まで、順次拡大していきます。
ただ、この自主点検も一度経験するとマンネリになるという傾向は否めません。そういう意味では、情報セキュリティとか、日本版ＳＯＸ法対応のように、いろいろな観点から問題が提起されるのは良いことだと思っています。それに基づいて強化していくことでさらに充実していくということかと思います。
また、この自主点検の詳細な内容は大切で、部門内でオープンにし共有化していくことによってリスク認識を共有化する上で有益ですし、ダイジェストを作って部門外にもわかりやすい資料とすることで、ＩＴ部門のリスク管理・内部統制の説明責任を果たしていく良いエビデンスになります。

次に、ＣＩＯインタビューで、よく耳にしたキーワードとして、監査人から「重箱の隅をつつく指摘」を受けているということがあります。先月も日経ビジネスで「すくむ経営」という記事が載りましたが、これからこうした事態が広がっていくと、日本の成長の阻害要因になっていくものと思います。
こうした新しいことでは、企業側の説明も不慣れでうまくいかないでしょうし、監査法人側もＩＴに関して知識が不十分な部分もあって、両者とも議論が噛み合わず悩んでいる状況だと思いますが、早い解決が必要だと思います。
ＣＩＯのインタビューの中で出てくる意見としては、「何も隠し事をする積りはなく、説明すること自体を拒否するものでは無いが、何しろ時間が惜しい」というのが、本音のようです。
或る企業では、説明する社員の時間を極力抑えたい、ワークロードや拘束時間を減らしたいということから、ＩＴの委託先で業務を知っているベテランに、監査法人からの基本的な質問を受けてもらうようにしている事例もあります。

■５－３　:内部統制を進化させていく仕組みを構築する。

私からのメッセージの３番目は、内部統制を進化させていく仕組みを構築するということであります。

先ほどのＣＩＯインタビューのときに、グローバル企業の動きを見ても、欧米の動きに連動していち早く活動をしていかなければならない時代になっているとお話ししました。

この日本と外国との差をどう認識するのかが、ますます重要になってきていると思います。

「内部統制進化論」、これは、ＷＥＢ進化論という言葉が出てきたときにすぐに引用しまして、日本はどれだけ米国から遅れているのか、ないしはどれだけ進んでいるのかという質問を投げかけて、今でも、皆でディスカッションをしています。

結果、皆さんの感じている温度差に驚きます。私としては、既に、スパイラルを回しながら、米国は進化していると受けとめていますし、ＣＯＳＯも 2004 年にＥＲＭへとレベルアップを図っています。逆に、この話をしたときに、「日本はスタート時点に立った」と表現したのですが、「それは、認識が甘いのではないか、日本はスタートに立っているのか、まだ立てずにマイナスの状態ではないのか」と言われて、厳しい見方ですけど現実はその通りかと思いました。

この進化をさせていく原点は何かということですが、「ノウハウの継承」にあると思います。皆さんが遭遇したリスク管理の一大事件は何かというと、Ｙ２Ｋであったと言えます。そのＹ２Ｋのノウハウを下地に積み重ねてきた企業は、いち早く進化を遂げています。

米国で、このノウハウが吸収され米国企業改革法の対応でも生かされている企業の例を聞き、日本の彼我の差の原点がここにあるのではないかと感じました。

先ほどの専門委員会・プロジェクトチームの話にまた戻りますが、テンポラリーまたは緊急対応のために編成し、ミッションが終われば解散する、そのこと自体に問題があるわけではありませんが、必ずそのノウハウを引き継いでいく仕組みを設けることが、大切です。

今回のインタビューで、委員会を設けていない企業に何故設けていないのかも聞きました。出てきた回答の中に、従来の組織でがっちりと対応できる、永続的に取り組む課題なので一時的な組織は作らないという回答がありました。立派な見識だと思います。

そして、ノウハウを継承しやすいものとするためには、標準化というステップも有効です。その時、そのときの対応ではなく、グローバルなスキームを取り入れてより汎用的なものにしておくことは、将来の負荷軽減には大切です。

■５－４ ： 経営との懸け橋となるシステムリスク管理の専門家を育成する。

私からのメッセージの最後である４番目は、人材育成と言う一番大きな課題についてです。

ＩＴ人材の育成が、ＣＩＯの最大の課題であるのと同じようにして、リスク管理の人材育成も喫緊の課題になっています。

リスク管理で求められるのは、システムの技術のみのプロではなく、複数の分野にまたがる事案を見る「複眼を持つ」人材であり、ビジネスプロセスを見渡せることが同様に大切になってきます。

このことで思いだすのは、昨年のカリフォルニア工科大学の卒業生の４分の１が、米国企業改革法対応の業務のために、コンサルタント会社に就職していったという話を同大学の一色教授からお聞きしたことです。

その時は、一過性のブームで、長続きをするとは思えないと冷ややかな気持ちで聞きましたが、最近一寸考えを改め始めています。

それは何かというと、経団連の高度ＩＴ人材育成という産学官合同で推進しているプロジェクトに関係していまして、その一環で九州大学工学部の大学院で講義を担当することになったのですが、先月、システムリスク管理からみた「企業の社会的責任とコンプライアンス」を講義したときに感じたことです。

このプロジェクトは、グローバル企業の新人を世界的に比較してみると、日本の大学を卒業した人達は３年ビハインドの位置にあるという事例等もあって、日本の将来を担うトップガンの精鋭を育成していかなければならないという危機意識から、活動がスタートしたわけです。

確かに専門分野の教育を強化しなければならないというのは事実であります。

しかし、それ以上に、経営的な見方も身につけてもらうことも大切で、こうしたテーマも組み入れることにした訳です。

今の世代の人達は、テレビゲームのＲＰＧで育ったこともあって、リスク管理で重要となるシナリオ分析でシミュレーションする感性は、むしろ磨かれているのかも知れないと思いました。

ＩＴ分野のベテランをリスク管理に投入するという手だけでなく、若い彼らの新しい感性をストレートにうまく育てていくことも、今後、この分野の人材を育成していく上で、大きな可能性があると思いました。

学生の育成から企業内の人材に話を戻しますと、リスク管理は孤独で理解してくれる人も少なく、孤独で疲れる業務なので、トップの支援が大切だと思っています。

内部統制というテーマの性格上、優秀で、なおかつきちっとした仕事をする人を割り当てていらっしゃるのですが、生真面目だと却って裏目に出てしまうことがあります。

先ほどのように、際限のない指摘がありますと、過剰反応して精神的な弱さが露呈しがちです。これが短期間ではなく、１年近く続くとなると、最近の若い人達は精神的に弱いという話がありますので、相当なストレスが溜まり心配です。
インタビューを終えるときには、部門長に、優秀な人材を守るために、愚痴・悩みを聞くなどのケアをしていく大切さを再認識して戴いています。
また、ＪＵＡＳの研究会も、悩みを一緒に解決する場として、役立てていきたいと思っています。
本日お集まりの方々は、責任あるポジションで関心もお持ちだと思います。自分の部下は当然として、社内・社外関係なく、数少ない日本の貴重な人材ですから、一緒に育てて、良い文化を作っていくことにご協力いただきたいと思います。

最後に、本日の私が申し上げたことのおさらいをして、この講演を終わりにしたいと思いましたが、これからパネルディスカッションがあるのに、この時点でおさらいするのは如何なものかという意見もありましたので、続く講演者の方の発表内容も反映させて、最後のパネルディスカッションでお話ししたいと思います。

以上、ご清聴ありがとうございました。
決して、一過性で終わるものではなく、企業が存続する限り続く永遠の課題です。
是非、「身の丈に合った」リスク管理・内部統制を実現してください。

（パネルディスカッションにおいて）

CIOはIT統制にどう取り組んでいるか

本日、基調講演で申し上げたことを、テーマである「ＣＩＯはＩＴ統制にどう取り組んでいるか」ということに即して、おさらいしておきます。

■５－１　CIOは　・・・　抱えている多岐に渉る経営課題を視野に入れて、「全体最適の仕組み」を考えることが求められている

経営課題は、常に複数あります。ブームのようにして、社会が注目して取り上げられる課題への対応は、確かに重要ではありますが、関連する経営課題と絡ませながら、経営として「元々やらなければならない課題」を実現すべく、工夫を重ねていくことが、最終的には、ＩＴ投資の有効性や真の解決に資するものと思います。

■５－２　IT統制とは　・・・　科学的なアプローチで経営の数値化を推進する

リスク管理の基本は難しくはありません。先ほど挙げたようなキーワード　「リスクベース・アプローチ」、「全体像を１枚で描く」、「素因数分解」、「数値化」等の基本的な考えを使って、分かり易い表現の仕方を工夫していくことです。

また、ＩＴ統制が、経営にとってだけでなく、現場の一線の方達にとっても受け入れられていくための重要なポイントは、不祥事件が起きた場合でも「説明責任を果たせて身を守れる」仕組みを構築していくことにあるということで、そのツールとしてＩＴは極めて有益であるということをよく理解してもらうことであると思います。

■５－３　取り組む・・・　自社の「身の丈に合った仕組み」を考える

盛んに開催されている講習会やセミナーでの情報を鵜呑みにして、自社に導入しようとしても、大量の輸血をするようなもので、経営も現場も担当者も拒否反応で病気になります。時間は余計にかかるかも知れませんが、自分の口から栄養のある食材を取って咀嚼して力をつけていくしかないと思います。

【補足】

１．何故、この概要をまとめたのか。

ご存知の方も多いと思いますが、ＭＩＴでは２千近い科目の講義の概要を大学のＨＰで無償公開していますし、日本でも、こうしたオープン化の動きが芽生え始めています。（http://ocw.mit.edu/index.html　http://www.jocw.jp/index_j.htm　等）

今回の講演の記録も、同じようにＨＰで情報発信することで、少しでも皆さんの認識を深めることに資するものがあればと思いました。

特に、「他の組織やベンダーに責任転嫁することなく、自ら果たすべき役割を認識し、肚に落として実行していくことの大切さ」、「人材不足が深刻な問題であり、広く施策を打っていくことの重要性」などを、ご理解いただけたら幸いです。

２．その後の動き。

講演（６月２０日）と現時点（７月１３日）で、異なっているのは以下の２点です。

◆ＣＩＯ論で発言を引用した東京海上日動火災の隅は、取締役社長に就任しました。

◆東京海上日動火災の持ち株会社のミレアホールディング社は、2007 年７月５日開催の取締役会で、ＮＡＳＤＡＱにおける米国預託証券の上場を自主的に廃止して店頭市場に移行させるとともに、ＳＥＣ登録廃止の申請を行うことを決議しました。